



## **An Immune Based Patient Anomaly Detection using RFID Technology**

Sri Listia Rosa<sup>1</sup>, Siti Mariyam Shamsuddin<sup>2</sup>, Evizal<sup>3</sup>

<sup>1,2</sup>Soft Computing Research Group, Faculty of Computer Science and Information System  
Universiti Teknologi Malaysia, 81310, Johor, Malaysia  
srilistia@gmail.com, maryam@utm.my

<sup>3</sup>Wireless Communication Centre, Faculty of Electrical Engineering  
Universiti Teknologi Malaysia, 81310, Johor, Malaysia  
evizal@gmail.com

### **ABSTRAKSI**

Mendeteksi anomali data pasien penting untuk memberikan kewaspadaan awal ke rumah sakit, dalam makalah ini akan membahas mengenai anomali mendeteksi data pasien dan pengolahan menggunakan sistem komputer cerdas buatan. Sistem Kekebalan Buatan (SKB) adalah sebuah teknik komputasi cerdas mengacu pada sistem imunologi manusia dan telah digunakan di banyak bidang seperti sistem komputer, pengenalan pola, perdagangan pasar saham, dan lain - lain. Dalam hal ini, nilai algoritma seleksi negatif nilai sebenar (RNSA) dari sistem kekebalan tubuh buatan yang digunakan untuk mendeteksi anomali parameter tubuh pasien seperti suhu. Data pasien dari sistem pemantauan atau basis data diklasifikasikan menjadi nilai sebenar dihargai, nyata hasil algoritma seleksi negatif adalah nilai sebenar daro nilai pemotongan oleh RNSA jarak, algoritma yang digunakan adalah jarak minimum dan nilai detektor dihasilkan untuk algoritma. Nilai sebenar dihargai dibandingkan dengan jarak data, jika jarak kurang dari detektor jarak RNSA maka data yang diklasifikasikan menjadi abnormal. Untuk mengembangkan mendeteksi waktu nyata dan memantau sistem, Identifikasi Frekuensi Radio (RFID) adalah teknologi Radio telah digunakan dalam sistem ini.

**Kata Kunci:** AIS, RNSA, RFID, Abnormal

### **ABSTRACT**

Detecting of anomalies patients data are important to gives early alert to hospital, in this paper will explore on anomalies patient data detecting and processing using artificial computer intelligent system. Artificial Immune System (AIS) is an intelligent computational technique refers to human immunology system and has been used in many areas such as computer system, pattern recognition, stock market trading, etc. In this case, real value negative selection algorithm (RNSA) of artificial immune system used for detecting anomalies patient body parameters such as temperature. Patient data from monitoring system or database classified into real valued, real negative selection algorithm results is real values deduction by RNSA

distance, the algorithm used is minimum distance and the value of detector generated for the algorithm. The real valued compared with the distance of data, if the distance is less than a RNSA detector distance then data classified into abnormal. To develop real time detecting and monitoring system, Radio Frequency Identification (RFID) technology has been used in this system.

**Keywords:** AIS, RNSA, RFID, Abnormal

## **1. INTRODUCTION**

Healthcare industry is under continuous development and improvement. Improving patient safety, nursing efficiency and quality of treatments brings productivity to separate healthcare processes. To achieve this, healthcare has turned towards IT and its applications, as these are noted to bring efficiency for healthcare professionals [1]. Components in a hospital for patient care such as facilities, equipments, management system, etc. One of component is patient monitoring system that can able to monitor patient parameters such as body temperature, blood pressure, body mass index, heartbeat. Currently most of hospitals use traditional system to check and monitor patient, by visiting patient to the ward or room to collect patient information. Manual or semi-auto system were used for record patient information, for example used manual temperature meter to measure patient body temperature and record in manual log, this method make patient uncomfortable and waste time for staff to visit and collect information. With technology development and requirement a hospitals have to provide good management system and service to customer or patient.

To improve healthcare and always notable patient safety, new systems and methods from the IT are deployed. Such as bar code medication administration, electronic health records systems and computerized provider order entry systems has been shown to enhance patient safety. Additionally, use of IT in different operations in a hospital environment is noticed to improve nursing efficiency and therefore decrease healthcare expenses [2-4]. Artificial Immune System (AIS) is a computational technique inspired by ideas coming from immunology and used to develop adaptive systems capable to solve different domain problems. AIS has recently become one of the most popular research tool studied and applied to solve problems in the field of computer security, in particular to detect computer viruses or intruders in computer networks, but also it has been applied to solve scheduling problem, build decision support systems or solve function optimization and combinatorial optimization problems [5-7].

Radio frequency identification (RFID) is a part of automatic identification, basically this technology founded since Second World War, where to identify soldier in air flight. RFID as Auto-ID technology which was first developed in 1980's. The technology acts as a base in automated data collection, identification and analysis systems worldwide. RFID has found its importance application in a wide range of markets including livestock identification and automated vehicle identification systems because of its capability to track moving objects. These automated wireless systems are effective method in manufacturing environments

where barcode labels with some limitation could not survive to implement. RFID grew drastically and popular almost in every application in late 1990's [8-9].

## 2. ARTIFICIAL IMMUNE SYSTEM

Artificial immune systems (AIS) are adaptive systems, inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving [6]. The field of artificial immune systems is concerned with abstracting the structure and function of the immune system to computational systems, and investigating the application of these systems towards solving computational problems from mathematics, engineering, and information technology. AIS is a sub-field of Biologically-inspired computing, and Natural computation, with interests in Machine Learning and belonging to the broader field of Artificial Intelligence [10].

Artificial immune systems have become known as an area of computer science and engineering that uses immune system metaphors for the creation of novel solutions to problems. Whilst this forms the majority view that the area of AIS is much wider and is not confined to the development of new algorithms. Previous research with this view and in fact goes onto define three types of AIS scientists [7]. The first are those of the "literal" school that build systems in silicon to try and do what the actual immune system does. Second is "metaphorical" school that look for inspiration from the immune system and build computational systems with the immune system in mind, and a third school of people who aim to understand immunity through the development of computer and mathematical models. Figure 1 shows antibody and antigen with Paratope, Epitope and Idiotope.

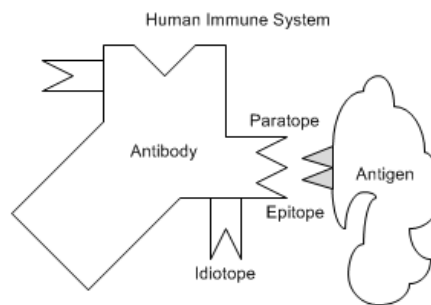


Figure 1. Antibody and antigen with paratope, epitope and idiotope

Biological immune in computer systems are serving as inspirations for a variety of computationally based learning systems (e.g., artificial neural networks and genetic algorithms). The immune system is comprised of several different layers of defence physical, physiological, innate (non-adaptive), and adaptive. The adaptive defence mechanism is sometimes referred to as acquired. Any action of the immune system against a pathogen is known as an immune response. The most basic defence mechanism is the skin. It serves as a physical barrier to many pathogens. For pathogens that elude the skin barrier, there are physiological barriers. Figure 2

shows an example of structure biological antibody [11]. Research on biological immune system for computer as shows, the research describes the human immune system and its functionalities from a computational viewpoint. The objective is to provide the biological basis for an artificial immune system, also serve to illustrate how a biological system can be studied and how inferences can be drawn from its operation that can be exploited in intelligent agents. Functionalities of the biological immune system for example content addressable memory; adaptation, and so on are identified for use in intelligent agents [12].

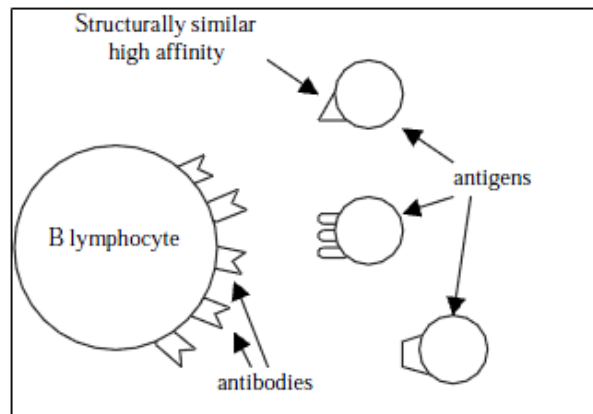


Figure 2. Antibody – antigen recognition and binding

Previous research on AIS as a hybrid immune learning algorithm presented, with the aim of combining the advantages of real valued negative selection algorithm (RNSA) and a classification algorithm. The basic idea is to use the RNSA algorithm to generate non-self samples. Then, apply a classification algorithm to find a characteristic function of the self (or non-self). The algorithm allows the application of a supervised learning technique even when samples from only one class (normal) are available. Another research on AIS applying innate immunity and dendritic cells concept for anomalies in real-time systems as [13], the challenging problem was solved using a combination of learning and evolution such that the framework can adapt to changing circumstances. This is in contrast to previous work in both the real-time systems and artificial immune systems where the knowledge has been determined statically off-line.

## 2.1 CLONAL SELECTION ALGORITHM

The clonal selection theory has been used as inspiration for the development of AIS that perform computational optimization and pattern recognition tasks. In particular, inspiration has been taken from the antigen driven affinity maturation process of B-cells, with its associated hyper mutation mechanism. These AIS also often utilize the idea of memory cells to retain good solutions to the problem being solved. There are two important features of affinity maturation in B-cells that can be exploited from the computational viewpoint. The first of these is that the proliferation of B-cells is proportional to the affinity of the antigen that binds it, thus the higher the affinity, the more clones are produced. Secondly, the mutations suffered by the antibody of a B-cell are inversely proportional to the affinity of the

antigen it binds [14]. In artificial immune systems, clonal selection algorithms are a class of algorithms inspired by the clonal selection theory of acquired immunity that explains how B and T lymphocytes improve their response to antigens over time called affinity maturation. The algorithms focus on the Darwinian attributes of the theory where selection is inspired by the affinity of antigen-antibody interactions, reproduction is inspired by cell division, and variation is inspired by somatic hypermutation. Clonal selection algorithms are most commonly applied to optimization and pattern recognition domains, some of which resemble parallel hill climbing and the genetic algorithm without the recombination operator [15].

## 2.2 NEGATIVE SELECTION ALGORITHM

The process of deleting self-reactive lymphocytes is termed clonal deletion and is carried out via a mechanism called negative selection that operates on lymphocytes during their maturation. For T-cells this mainly occurs in the thymus, which provides an environment rich in antigen presenting cells that present self-antigens. Immature T-cells that strongly bind these self-antigens undergo a controlled death (apoptosis). Thus, the T-cells that survive this process should be uncreative to self-antigens. The property of lymphocytes not to react to the self is called immunological tolerance [16]. Negative selection algorithms are inspired by the main mechanism in the thymus that produces a set of mature T-cells capable of binding only non-self-antigens. The first negative selection algorithm was proposed [17], to detect data manipulation caused by a virus in a computer system. The starting point of this algorithm is to produce a set of self-strings,  $S$ , that define the normal state of the system. The task then is to generate a set of detectors,  $D$ , that only bind/recognize the complement of  $S$ . These detectors can then be applied to new data in order to classify them as being self or non-self.

## 2.3 REAL-VALUED NEGATIVE SELECTION

The negative selection algorithm (NSA) is one of the most widely used techniques in the field of artificial immune systems. NSA used to detect changes in data behavior and patterns of raw data, by generating detectors in the complementary space. Originally detectors are used directly to classify new data as self (normal) or non-self (abnormal). Previous research in [18], proposed a real valued negative selection (RNSA) algorithm based on heuristics that try to distribute the detectors in the non-self-space in order to maximize the coverage. The method used algorithm a real-valued representation for the self/non-self-space that differs from the binary representation used in original negative selection algorithms. RNSA with higher-level representation able to provides some advantages such as increased expressiveness, the possibility of extracting high-level knowledge from the generated detectors and in some cases improved scalability. The real algorithm does not need to convert raw data to others scale or binary representation, it is use real data value to process and matching to a detector generated by using minimum distance [19]. Minimum distance valued set according to the high and low data received from the system.

### **3. PATIENT MONITORING SYSTEMS FOR ANOMALY DETECTION**

In today's healthcare practice, physicians have a need to monitor more than one medical parameter for patients that are either hospitalized or leading their normal daily activities at home or at work but in need of constant medical care. These patients, in turn, need a device that is easy to use, cost-effective and reliable to provide them with vital data about their medical condition. Such device should allow physicians to view the measured parameters over a long period of time for parameter or daily activities correlation and trend analysis. Patient monitoring system is one of component that aid healthcare industry to monitor patient, monitoring patient body parameters such temperature, blood pressure, heartbeat is helping doctor in diagnosis. Previous research is as presented in [20], where the application for Orthopaedics, wireless communication system based on wireless sensor network (WSNs), an array of inertial measurement units (IMUs) combined with ultrasound sensing provides a radiation free method to monitor in-vivo motion (e.g. bones in the knee); or a network of sensors to detect abnormal motions or vibrations for remote patient monitoring. Early detection of over patient and handling of alert and warning in such situation is essential to avoid malfunctioning and fatal in life of things. Anomaly detection technique in the patient monitoring in some applications are very important to give aware by others, else fatal and critical situation happen to the patient.

The anomaly detection problem can be stated as two-class classification problems, given a state of the system, classify it as normal or abnormal. There are many approaches to anomaly detection. A simple approach is to specify a range of variability for each parameter of the system. If the parameter is out of the range, it is considered as an abnormality. The most common approach uses a statistical model to calculate the probability of the occurrence of a given value, the less the probability the higher the possibility of an abnormality [21]. However, the statistical approach models individually the different variables that represent the state of the system, and ignores the fact that the notion of normalcy depends on correlation among different parameters, which could make it difficult to detect multivariable temporal pattern. Some approaches try to build modes based on the present and past states to predict the future states of the system.

#### **3.1 PATIENT TEMPERATURE MONITORING SYSTEM**

Temperature is a continuous variable that can be accurately measured and analyzed quantitatively. However, in clinical practice it is primarily used as an intermittent qualitative variable with often a poorly defined cut-off point. Despite its potential as a non-invasive physiologic signal to continuously assess patient status, its clinical use is often limited to a simple binary decision. Automatic temperature logging systems do not require manual intervention; instead they periodically log the temperature themselves. This has the considerable benefit of reducing the amount of work required to run a temperature logging system. In addition, larger temperature logging systems, usually using environment monitors, can be constructed that are able to measure the temperature in many separate locations. One of factor to keep automatic temperature logging system is the importance is data backup, especially if the system is being constructed for regulatory compliance reasons [22].

Normal human body temperature is a concept that depends upon the place in the body at which the measurement is made, and the time of day and level of activity of the person. There is no single number that represents a normal or healthy temperature for all people under all circumstances using any place of measurement. Different parts of the body have different temperatures. Measurements taken directly inside the body cavity are typically slightly higher than oral measurements, and oral measurements are somewhat higher than skin temperature. The commonly accepted average core body temperature (taken internally) is  $37.0^{\circ}\text{C}$  ( $98.6^{\circ}\text{F}$ ). The typical oral (under the tongue) measurement is slightly cooler, at  $36.8 \pm 0.7^{\circ}\text{C}$ , or  $98.2 \pm 1.3^{\circ}\text{F}$ . In samples of normal adult men and women, the observed range for oral temperature is  $33.2\text{--}38.2^{\circ}\text{C}$  ( $92\text{--}101^{\circ}\text{F}$ ).

### 3.2 REAL TIME MONITORING SYSTEM USING RFID TECHNOLOGY

Many solutions have been developed to alleviate the management issues in hospital for better services to the customers. In terms of monitoring human body temperature, nurse used traditional method with manual system to measure body temperature accordingly. However, this device has some weaknesses such as waste time to visit patient, use manual record and less accuracy. Hence, there are many alternative solutions have been developed to lessen the above issues. One of such solutions is using machine learning methods such as artificial neural network, fuzzy logic, support vector machine, and others in detecting the abnormal human body temperatures. However, recently artificial immune system (AIS) has been an inspiring solution in solving complex problems. Real time systems are traditionally associated with safety critical or high integrity applications, where incorrect behavior cannot be tolerated as it may result in catastrophic consequences. In addition, a large number of systems exist where real-time properties are desirable, although the failure to meet these will not have the same server consequences.

In order to create more efficient healthcare processes, IT and its use in healthcare has been studied extensively. One promising technology that can be used to both streamline processes and make them more secure is the RFID technology. It can be used for many operations in healthcare patient identification, material identification, equipment identification, device identification, medication identification, access control, and location and information transmission. Ultimately, the technology increases patient safety and brings efficiency for work of healthcare professionals. It can be noticed that most of the systems are focusing on patient identification [23]. Research on application RFID technology on healthcare industry as mention in [24], the RFID technology is a growing phenomenon among separate automated identification technologies. As a technology, it is used from the early 1940's, but just in the last decade, the IT (information technology) community and the healthcare sector have been taking more action on studying and developing the technology to correspond their requirements and needs. This paper represents a short overview of the RFID technology in healthcare. The paper focusing on the RFID technology, how it is used in different parts of healthcare and what kinds of results have been found.



**Sri Listia Rosa, Siti Mariyam Shamsuddin, and Evizal**  
**AnImmune Based Patient Anomaly Detection using RFID Technology**

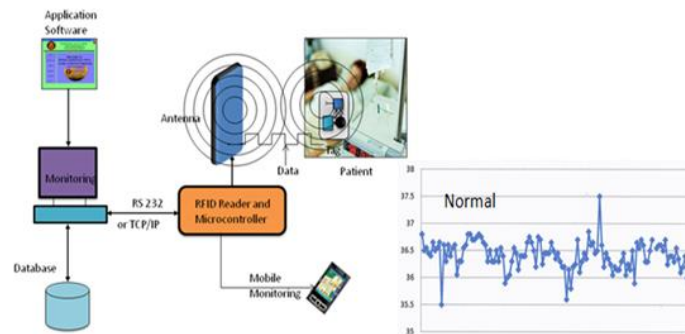


Figure 3. A real time patient temperature monitoring system

Lately many applications using RFID technology because of its advantages, this technology as a wireless system also the tag can be embedded with any sensor, for healthcare industry application such as embedded with human body temperature sensor, blood pressure, heartbeat, etc. Figure 3 shows an example of a real-time wireless temperature monitoring system for a patient; the signal is sent every 10 seconds. The sensor is used as an RFID tag with an embedded temperature sensor and sends information wirelessly to a backend system. The base receiver above the picture will pick up the signal and show it on your computer monitor screen. Wireless transmission distance between the transmitter and the receiver is about 80 meters line of sight and up to 50 meters indoors.

### 3.3 ANOMALY DETECTION TECHNIQUE

Traditionally, an anomaly detection technique treats data as a collection of multivariate records. A large and diverse literature on techniques that handle such data exists and has been covered in several survey articles and books. The literature on anomaly detection techniques for sequence data in healthcare application is relatively sparse. The importance of anomaly detection is due to the fact that anomalies in data translate to significant actionable information in a wide variety of application domains. For example, an anomalous traffic pattern in a computer network could mean that a hacked computer is sending out sensitive data to an unauthorized destination [25]. Anomaly detection used in computer security as shown in previous research is to provide a detailed example of a host-based intrusion detection system that monitors file systems to detect abnormal accesses. The file wrapper anomaly detector (FWRAP) has two parts, a sensor that audits file systems, and an unsupervised machine learning system that computes normal models of those accesses. The detector is first trained by operating the host computer for some amount of time and a model specific to the target machine is automatically computed; the model is then deployed to a real-time detector [26]. Anomaly detection refers to the problem of finding patterns in data that do not conform to expected behaviour. These non-conforming patterns are often referred to as anomalies, outliers, discordant observations, exceptions, aberrations, surprises, peculiarities or contaminants in different application domains. Of these, anomalies and outliers are two terms used most commonly in the context of anomaly detection; sometimes interchangeably. Anomaly detection finds extensive use in a wide variety



of applications such as fraud detection for credit cards, insurance or health care, intrusion detection for cyber-security, fault detection in safety critical systems, and military surveillance for enemy activities.

There is another previous research on anomaly detection, the work compare approaches to performing fully-distributed anomaly detection as a means of detecting security threats for objects equipped with sensing and communication abilities. With the desirability of increased visibility into the cargo in the transport chain and the goal of improving security, consider the approach of equipping cargo with sensing and communication capabilities as a means of ensuring the security of the cargo as a key application. real sensor test data from a rail trial and used the collected data to test the feasibility of the anomaly detection approach [27].

### 3.3.1 Real Valued Negative Selection Algorithm

Raw data that collected and before proceed into an algorithm, it should be collected, inspected, cleaned and selected. If the best detector fail in the detection of bad data, it's crucial for the data quality. Besides, since a detector can exploit only certain data features, it is important to decide which data presentation work best. RNSA requires that data to be divided into several group such as candidate detectors, self data and test data. Moreover, RNSA uses distance matching rules to generate detectors, thus the data obtained need to be converted into a format that most suits the algorithm's need. Basically, RNSA is divided into two phases, namely classification phase and monitoring phase. In the first phase, a set of detectors is generated and in the second phase, the new patient data is monitored by comparing them with the generated detectors. The strings is said to match each other if they fulfil the requirement of the selected matching techniques [28].

Previous author propose an algorithm based on the real-valued negative selection heuristic research to explore and try to distribute sensors in a non-self space to maximize coverage [26]. The algorithm uses a representation of the actual worth of their own space or non-self that is different from the binary representation used in the original negative selection algorithm. Representation of the higher level provides several advantages such as increased expression, the possibility of extracting high-level knowledge of detectors produced, and in some cases, better scalability. Figure 4 shows the flow chart of the negative selection algorithm implementation actual or real value.

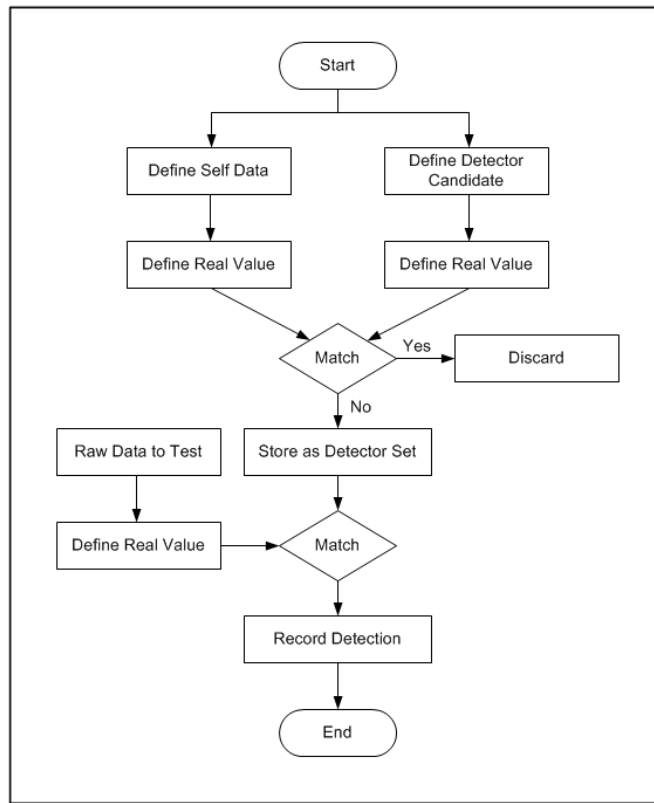


Figure 4. Implementation flowchart of RNSA

In this research attempts to empirically evaluate and observe the performance of real-valued negative selection algorithm of artificial immune system using minimum distance matching techniques in classification and monitoring of patient data in temperature. The comparison criteria are as follows:

- Number of detectors generated
- Detection accuracy
- Processing Time

The results obtained from the experiments and testing are compared in terms of number of the detectors generated in the classification phase, the processing time of the matching process and the accuracy of the experiment output. Figure 5 illustrates the proposed framework for abnormal patient temperature monitoring using RNSA. The proposed framework of the detector set generation phase can be summarized as follow:

1. Define historical patient data as real valued
2. Generate candidate of detectors
3. Enough of number detectors, if no generate more detectors
4. If new detectors if accepted, define as detector set else discharge for as detectors.  
 Detector set (R) store for matching to the live patient data.

After generating the set of detectors  $R$ , the next stage of the algorithm is responsible for monitoring the system for the real valued of data, which is the test data in this study. The test data monitoring phase can be summarized as follow

1. The patient data is presented to the system
2. Compare (match) the test data with the detector set  $R$
3. If match occurs, for example, if an element of test data is recognized by an element of detector set  $R$ , then non-self data, which is abnormal temperature data, is detected.

If a non-self-data is recognized, an action has to be taken. The resulting action of detecting non-self-varies according to the problem under evaluation. In this research, a warning will be triggered so that immediate actions will be taken to see patient and checking.

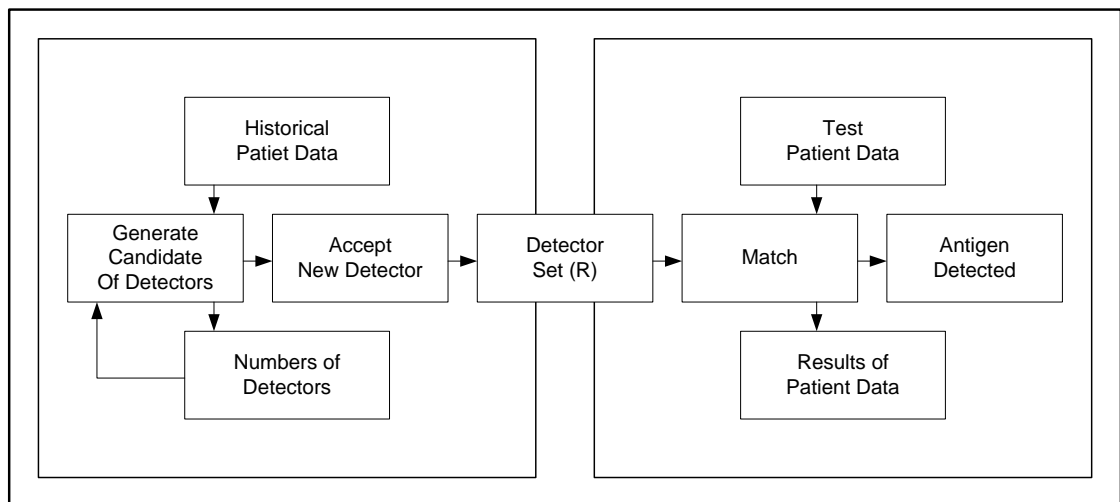


Figure 5. Proposed frameworks for abnormal patient body detection using RNA

### 3.3.2 Patient Data Presentation

Data processing in real terms, the selected input data collected from the database and the system is a binary format. Data presentation using the algorithm options negative return value (RNA) or R-NSA based on heuristics that try to distribute sensors in a non-self space to maximize coverage. This algorithm uses the actual value representation for self / non-self space which is different from the binary representation used in the original negative selection algorithm[29]. In the presentation of this data to the original data is not encoded binary format, but all the data is processed in real value. Both of these data will be compared between each other using a detector with a minimum distance technique, if the data selection algorithm significantly less than the value of sample data will then cause abnormal and vice versa when the negative selection algorithm significantly larger than the data sample of the output data will be normal conditions. Pseudo code to show data with negative selection algorithm as shown below, where MaxSelfData is 100,

**Sri Listia Rosa, Siti Mariyam Shamsuddin, and Evizal**  
**AnImmune Based Patient Anomaly Detection using RFID Technology**

MaxDetector 300 and minimum values for the minimum distance is 0.05. The purpose of using the minimum distance to compare the sample to the detector data generated.

*Class Main Form*

```
Function Initialize()  
    NSA nsaAlgorithm = new NSA()  
    nsaAlgorithm.MaxSelfData = 100  
    nsaAlgorithm.MaxDetector = 300  
    nsaAlgorithm.MinDistanceValue = 0.05  
    nsaAlgorithm.CreatedSelfData()  
    nsaAlgorithm.CreateDetector()  
End Function  
Function Button_Click(BMIValue)  
    NormalizedBMIValue = nsaAlgorithm.Normalize(BMIValue)  
    DetectedValue = nsaAlgorithm.Detect(NormalizedBMIValue)  
    If DetectedValue == 1 Then  
        NORMAL  
    Else  
        ABNORMAL  
    End If  
End Function  
End Class  
Class
```

#### 4 EXPERIMENT AND IMPLEMENTATION

Radio frequency identification (RFID) technology is used for anomaly detection system of the patient and the use of this technology because of several advantages to this system. A RFID tag with a temperature sensor attached to the patient's body and gathering by the tag as the body temperature of patients sent to the RFID reader wirelessly. RFID reader receive all the informations of the number of patients (tag) and each patient has a unique ID to distinguish each other patients, information processing will be done in the microcontroller attached to the reader. Figure 6 shows a block diagram RFID system with some tags attached to patients and collecting patients body temperature data. System able to cater a few tags and collect data that sends to backend system to process.

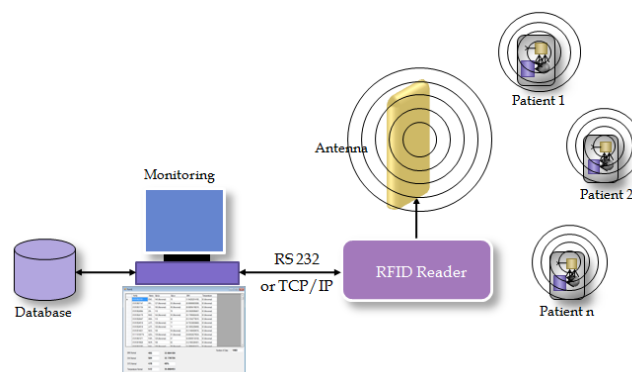


Figure 6. Blok diagram of RFID system for collecting patient's data

Data with patient ID and information send to the backend system (database) for documentation and analysis, the system analyzes the patient's underlying abnormalities in the received data. Figure 7 shows the hardware part called RFID reader with embedded chip as a microcontroller to process the data received from the sensor (tag). Negative real value selection algorithm is used to a method for processing data test abnormalities, techniques and methods are to execute the hardware. In order to perform in real life and to test the real data, the hardware will need to adopt proposed algorithm.

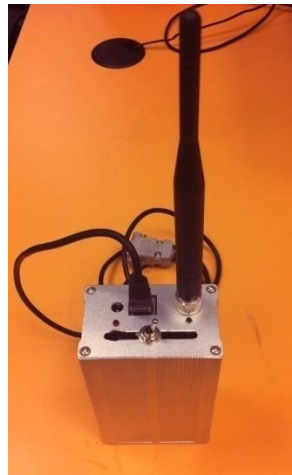
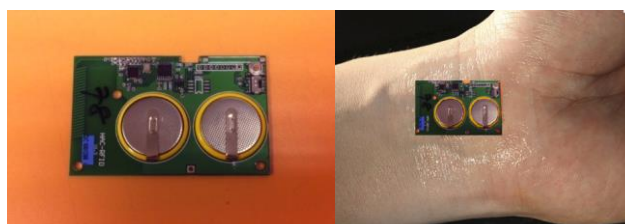


Figure 7. Active RFID reader

In the actual sample data, test data obtained by the experiment several patient samples and test them is in the range of the body temperature, to optimize the analysis of this sample data requires as much as possible. Fig. 8 shows the example of data collection of patient's body temperature. Figure 8 (a) A RFID with embedded temperature sensor and Figure 8 (b) A patient with RFID tag attached to the body for body temperature collection, all patients had a record of information as body temperature and send the information to a database for analysis. In a real scenario, clinic or hospital that received number of patients data will check every day with this system, how many patients with normal or abnormal body parameters than doctor or hospital will know and can take some intensive inspection or action.



(a)

(b)

Figure 8.(a) RFID tag with temperature sensor (b) Data collection

Experiments process divided into two phases, the classification phase and monitoring phase. In the classification phase detector dataset itself and the candidate will undergo a matching process to generate a set of detectors. In matching techniques used are real valued negative selection algorithm. Detector set generated in phase monitoring will be carried forward to the next phase for monitoring purposes. In the monitoring phase, the set of sensors and test data will be presented as input to the matching process. There are two sets of test data used to test whether the experiment can produce a desired output. The first set of test data consisting of real patient data and the second set consists of test-added data anomalies. Similarly, the matching techniques used are real valued negative selection algorithm. If a match is found between the detector and the test data set, the system will notify the user of abnormal detection. In order to evaluate the performance of different matching techniques, the results of the experiment than in the long number generated detectors, the time required for matching process and accuracy of detection. Figure 9 shows an overview describes in detail the process of experiment, in which the actual value and the minimum distance is used in the classification phase for adaptation techniques.

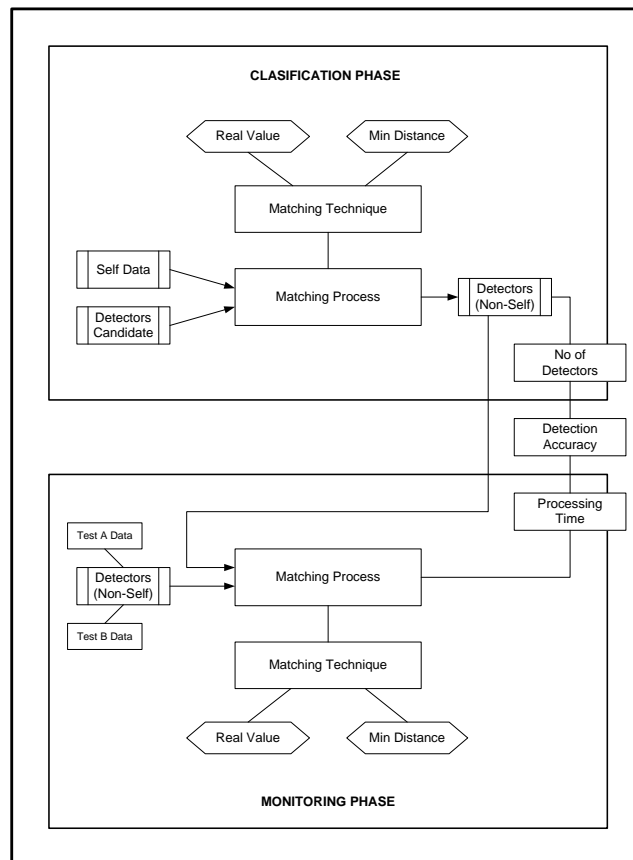


Figure 9. An overview of the experimental process

In the experiment process, two sets of test data were used in the monitoring process in order to detect whether tested data consist of abnormality patient data detected. For the first test data is use of live data patient body temperature and follow by scenario of anomaly data collected. The first test data is made up of the real stock data and the second test data composed of anomaly added data. The quantity of source data distribution is shown in Table 1.

Table 1. Quantity of data distribution

Patient Data	No of Detector	No of Self Data	Test Data 1	Test Data 2
Body Temperature	100 - 300	1460	570	890

Test data in this experiment used real-valued matching technique of negative selection process on the selected data; the experiments are conducted on each dataset. For matching technique, use minimum distance for the matching with the value is 0.05 and compare to the data set. Each data set does not convert to other value or parameter, the data set use real-valued to process. All the experiments are tested on two set of data, where the first test data is made up of the real patient data and the second test data composed of anomaly-added data. Table 2 shows the number of abnormal data added in second test of each data set.

Table 2. No of anomalies data added in second test of data set

Data Set	No of Anomaly Added
Body Temperature	114

## 5 RESULT AND DISCUSSION

Distribution of human body temperature is different in every part of the human body, some of which represent the major human body temperature monitoring that can be used for reference shown as part of it. One of the human body that can monitor the temperature of the human body is the skin of hands, the temperature at lower today consider the human body temperature outside. Normal internal body temperature is 35-38 degrees Celsius and the outside is 29-36 degrees Celsius. Figure 10 shows some of the data collected human body temperature during the period January 2010 to December 2011.



**Sri Listia Rosa, Siti Mariyam Shamsuddin, and Evizal**  
**AnImmune Based Patient Anomaly Detection using RFID Technology**

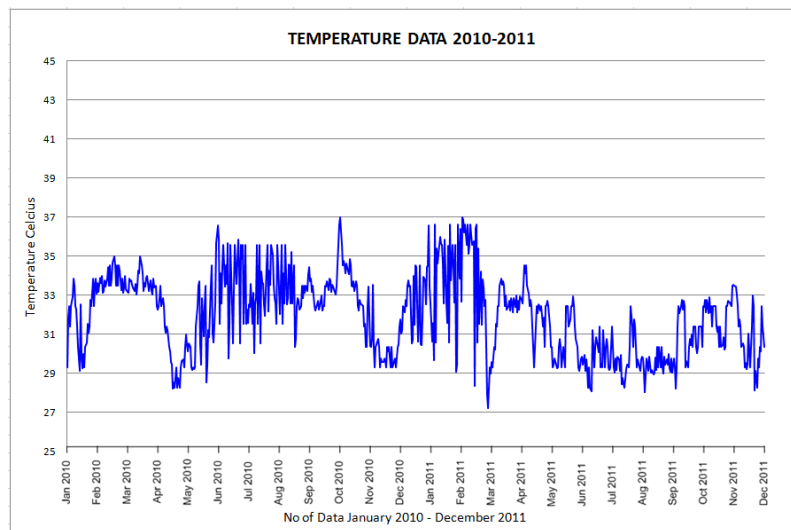


Figure 10. Set of body temperature data from 2010 to 2011

Table 3 shows the results of classification and performance monitoring human body temperature recorder. The real value of negative selection algorithm with different numbers of detectors used for testing. In a test conducted some repetition with different values of the number of detectors, detector used ranging from 100 to 300. The results of all test data shown in Table 3 which represents the test data abnormal detected. In this experiment to assess the ability of each technique that matches the classification and monitoring tasks. Number of detected abnormal data is from 93 to 115 for the number of different sensors. The comparison is based on the number produced in the phase detector classification and comparison in the match, and the time required for matching process and produce results is average 1 second.

Table 3. Numbers of abnormal data in first experiment

Experiment	No of detector	Processing time	Result
1	100	1 sec	93 abnormal data detected
2	120	1 sec	95 abnormal data detected
3	140	1 sec	96 abnormal data detected
4	160	1 sec	98 abnormal data detected
5	180	1 sec	98 abnormal data detected
6	200	1 sec	101 abnormal data detected
7	220	1 sec	105 abnormal data detected
8	240	1 sec	107 abnormal data detected
9	260	1 sec	110 abnormal data detected
10	280	1 sec	112 abnormal data detected
11	300	1 sec	115 abnormal data detected

To test patient temperature data obtained in 2010 to 2011, the first test performed for the total number of data of 570 patients'. This test is the first of two sets of data, then to be compare to the results of the tests carried out with the actual

value of abnormalities found in the dataset. As shown in Table 3 above, to graph comparison with the actual value of abnormalities data such as depicted in Figure 11 below, the number of detector used in testing is starting from 100 to 300. Value obtained from the analysis of patient data abnormalities that is 105, the actual value of this approach abnormal patient data, that mean number of detector mathing for this sample test data experiment is 220.

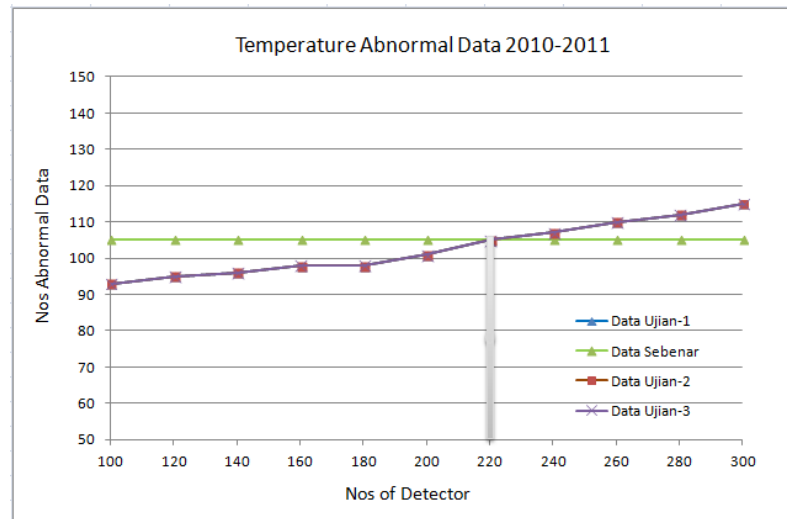


Figure 11. Comparison body temperature abnormal data 2010 to 2011

Figure 12 shows the set temperature of the human body for the period January 2011 to December 2012. All data sets are tested as previous methods for algorithm variants using real-valued negative selection. Human body temperature experiments performed to test the second data collected dataset for 2011 to 2012 based on the detection of the data collected.

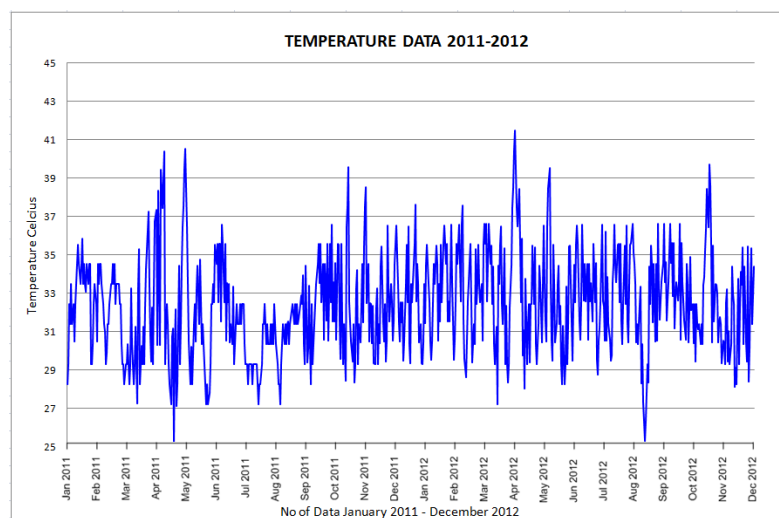


Figure 12. Set of body temperature data from 2011 to 2012

**Sri Listia Rosa, Siti Mariyam Shamsuddin, and Evizal**  
**AnImmune Based Patient Anomaly Detection using RFID Technology**

Temperature data collected human body consists of 790 data sets. Similar to previous test, the data are divided into two groups which is the data set for detection and test data, 2011 data into a set of sensors and the second test data used all data 2011 to 2012. Table 4 shows the classification and monitoring the performance of the actual value of negative selection algorithm with a different tracking number, as all test data is done several times with the detection of 100 to 300 as in the previous tests. Refer to the test results in a number of abnormal data is 114 detected. The results of all test data are shown in the table below, represents the number of data abnormality is detected, this indicates that the human body temperature data in abnormal or pain. Time to process all the data as usual testing that occurred in the previous test that is average in 1 second, this means considered reasonable time for system to analyze.

Table 4. Numbers of abnormal data in second experiment

Experiment	No of detector	Processing time	Result
1	100	1 sec	107 abnormal data detected
2	120	1 sec	107 abnormal data detected
3	140	1 sec	108 abnormal data detected
4	160	1 sec	110 abnormal data detected
5	180	1 sec	112 abnormal data detected
6	200	1 sec	114 abnormal data detected
7	220	1 sec	114 abnormal data detected
8	240	1 sec	117 abnormal data detected
9	260	1 sec	118 abnormal data detected
10	280	1 sec	120 abnormal data detected
11	300	1 sec	121 abnormal data detected

Figure 13 below shows a comparison number of data and number of abnormal data detected by detectors, refer to the test results by the number of the second set of data that is 890 sample. In accordance with the test results obtained with the detection of the real value is for tracking the number of 200 to 220. Which mean value of datector from 200 to 220 is suitable for this experimet of test data.

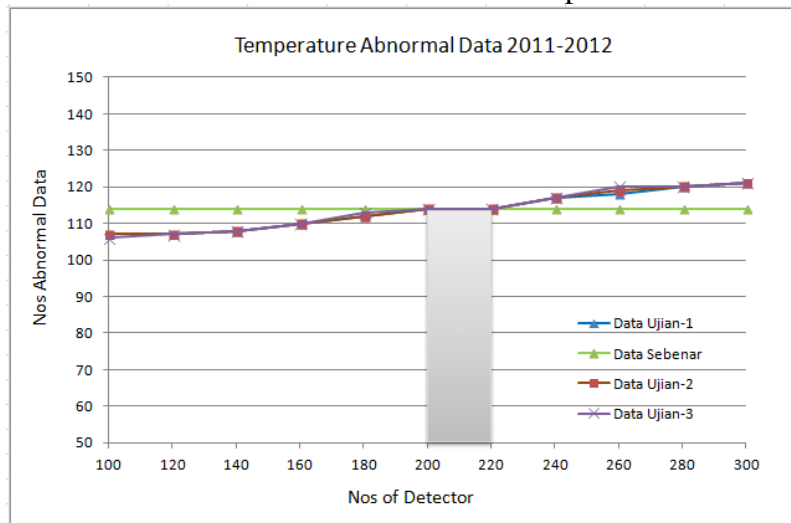


Figure 13. Comparison body temperature abnormal data 2011 to 2012

## 6 CONCLUSIONS

In this research, experiments, tests and practical investigation of artificial immune system application in healthcare industry investigated. Patient data and live collecting from patients have been done for detect anomalies of data. Accuracy of anomalies data detected to be one of the concerns in this experiment and the challenge to the system because a large amount of patient data. Several tests and experiments were conducted to evaluate the performance of selected systems and good pitching technique. The real value of the negative selection algorithm selected to detect this error, which collect patient data in real and direct analysis to detect anomalies data. This study focused on patients' data on body temperature.

Large amount of patient data collected directly from used in experiment and test the validity of the actual value of the negative selection algorithm. Minimum distance matching techniques are used to compare and find anomalies data, some of the data generated and compare to test data to find anomalies. The results showed that the minimum distance matching techniques to find data anomalies with a large number of test data. Overall, this study proves that the real value of negative selection algorithm with a minimum distance technique has the potential to be used as a tool to detect anomalies in the patient data in the healthcare industry, particularly in the hospital or clinic.

## REFERENCES

- [1] R. a. S. Perrin, N., "RFID and Bar Codes Critical Importance in Enhancing Safe Patient Care," *Journal of Healthcare Information Management*, vol. 18(4), pp. 33-39, 2004.
- [2] R. Kaushal and D. W. Bates, "Information technology and medication safety: what is the benefit?," *Quality and Safety in Health Care*, vol. 11, pp. 261-265, September 1, 2002 2002.
- [3] E. Oren, *et al.*, "Impact of emerging technologies on medication errors and adverse drug events," *American Journal of Health-System Pharmacy*, vol. 60, pp. 1447-1458, July 1, 2003 2003.
- [4] L. E. MOODY, *et al.*, "Electronic Health Records Documentation in Nursing: Nurses' Perceptions, Attitudes, and Preferences," *Computers Informatics Nursing*, vol. 22, pp. 337-344, 2004.
- [5] P. B. Jon Timmis, Emma Hart, "Artificial immune systems " *second international conference, ICARIS, Edinburgh*, 2003.
- [6] L. R. d. Castro and J. Timmis, *Artificial Immune Systems: A New Computational Intelligence Paradigm*: Springer-Verlag New York, Inc., 2002.
- [7] J. Timmis, Neal, M., Hunt, J. , "An Artificial Immune System for Data Analysis," *Biosystems*, vol. 55, pp. 143-150, 2000.
- [8] K. Finkenzeller, in *RFID Handbook*, ed: John Wiley & Sons, Ltd, 2003.
- [9] A. Lahtela, "A Short Overview of the RFID Technology in Healthcare," presented at the Proceedings of the 2009 Fourth International Conference on Systems and Networks Communications, 2009.

- [10] J. Timmis, *et al.*, "Immune Systems and Computation: An Interdisciplinary Adventure," in *Unconventional Computing*. vol. 5204, C. Calude, *et al.*, Eds., ed: Springer Berlin Heidelberg, 2008, pp. 8-18.
- [11] R. L. King, *et al.*, "The Biological Basis of the Immune System as a Model for Intelligent Agents," presented at the Proceedings of the 11 IPPS/SPDP'99 Workshops Held in Conjunction with the 13th International Parallel Processing Symposium and 10th Symposium on Parallel and Distributed Processing, 1999.
- [12] H. Lu, "Artificial Immune System for Anomaly Detection," in *Knowledge Acquisition and Modeling Workshop, 2008. KAM Workshop 2008. IEEE International Symposium on*, 2008, pp. 340-343.
- [13] N. Lay and I. Bate, "Applying artificial immune systems to real-time embedded systems," in *Evolutionary Computation, 2007. CEC 2007. IEEE Congress on*, 2007, pp. 3743-3750.
- [14] L. N. d. Castro and F. J. V. Zuben, "The Clonal Selection Algorithm with Engineering Applications 1," presented at the Genetic and Evolutionary Computation Conference, 2000.
- [15] F. Burnet, "A modification of Jerne's theory of antibody production using the concept of clonal selection," *CA: A Cancer Journal for Clinicians*, vol. 26, pp. 119-21, 1976.
- [16] K. Igawa and H. Ohashi, "A negative selection algorithm for classification and reduction of the noise effect," *Appl. Soft Comput.*, vol. 9, pp. 431-438, 2009.
- [17] H. Wang, *et al.*, "PSO-Optimized Negative Selection Algorithm for Anomaly Detection," in *Applications of Soft Computing*. vol. 52, E. Avineri, *et al.*, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 13-21.
- [18] F. González, *et al.*, "A Randomized Real-Valued Negative Selection Algorithm," in *Artificial Immune Systems*. vol. 2787, J. Timmis, *et al.*, Eds., ed: Springer Berlin Heidelberg, 2003, pp. 261-272.
- [19] J. Hunt, *et al.*, "Jisys: Development of an artificial immune system for real world applications," in *Artificial Immune Systems and their Applications*, ed: Springer, 1998, pp. 157-186.
- [20] R. C. Wasielewski, "Wireless technologies for the orthopaedics: Diagnostics and surgical applications," in *Biomedical Wireless Technologies, Networks, and Sensing Systems (BioWireless), 2011 IEEE Topical Conference on*, 2011, pp. 1-2.
- [21] M. Cai, "A Novel Immunity-Based Model for Anomaly Detection," presented at the Proceedings of the 2008 International Conference on Computer Science and Software Engineering - Volume 03, 2008.
- [22] M. C. Varela, M.; Chana, M.; Gomez-Mestre, I.; Asensio, R.; Galdos, P., "Clinical implications of temperature curve complexity in critically ill patients," *Crit. Care Med*, vol. 12, pp. 2764-2771, 2005.
- [23] C. Yu, *et al.*, "Design of Clinic Patient Body Temperature Wireless Remote Concentration Monitor System Based on VI," in *Education Technology and Computer Science, 2009. ETCS '09. First International Workshop on*, 2009, pp. 630-634.
- [24] T. Landolsi, *et al.*, "Wireless stand-alone portable patient monitoring and logging system," *Journal of Communications*, vol. 2, pp. 65-70, 2007.

- [25] S. Stolfo, *et al.*, "Anomaly Detection in Computer Security and an Application to File System Accesses," in *Foundations of Intelligent Systems*. vol. 3488, M.-S. Hacid, *et al.*, Eds., ed: Springer Berlin Heidelberg, 2005, pp. 14-28.
- [26] F. Gonzalez, *et al.*, "Combining negative selection and classification techniques for anomaly detection," in *Evolutionary Computation, 2002. CEC '02. Proceedings of the 2002 Congress on*, 2002, pp. 705-710.
- [27] M. Gong, *et al.*, "Short Communication: An efficient negative selection algorithm with further training for anomaly detection," *Know.-Based Syst.*, vol. 30, pp. 185-191, 2012.
- [28] J. Sifakis, *et al.*, "Building models of real-time systems from application software," *Proceedings of the IEEE*, vol. 91, pp. 100-111, 2003.
- [29] J. Timmis and M. Neal, "A resource limited artificial immune system for data analysis," *Knowledge-Based Systems*, vol. 14, pp. 121-130, 2001.

**Sri Listia Rosa, Siti Mariyam Shamsuddin, and Evizal**  
**AnImmune Based Patient Anomaly Detection using RFID Technology**